UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/718,663 | 11/24/2003 | Jun Furukawa | Q78522 | 1253 |

23373 7590 09/10/2007

SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

| EXAMINER | |
|---|---|
| PARTHASARATHY, PRAMILA | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2136 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 09/10/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

mn

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/718,663 | FURUKAWA, JUN | |
| | Examiner | Art Unit | |
| | Pramila Parthasarathy | 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *29 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/29/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

**1.** This action is in response to the communication 04/29/2004. No preliminary amendments to the claims were filed. Claims 1 – 11 are currently pending.

### *Priority*

**2.** Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged.

### *Information Disclosure Statement*

**3.** An initialed and dated copy of Applicant's IDS form 1449 is attached to the Office action.

### *Double Patenting*

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., In re Berg, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

**4.** Claims 1 – 11 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 – 53 of U.S. Patent No. 7,003,541. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1 – 11 correspond to the claims of 1 – 53 of the patent claims, except in the instant claims the elements "a proof system comprising a prover supplied with a first random tape and a verifier supplied with a second random tape, wherein the prover communicates with the verifier to prove that the prover has a witness comprising: a generator supplied with a third random tape ... a simulator with a fourth random tape, a distinguisher supplied with a fifth random tape, wherein the generator supplies the common input to the prover, the verifier, the simulator and the distinguisher ...the distinguisher evaluates the proof system .... and computationally indistinguishable for at least one of possible common inputs" is referred in the patent claims as "a first mechanism for proving equality or inequality of two discrete logarithms and a second mechanism for verifying said equality or inequality, wherein ... a random number generator for generating a first random number ... proving section for proving equality of a discrete logarithm ...a verifying section corresponding to the proving section for verifying equality of a discrete logarithm ... a checking section for checking the received random input ....a decision section for deciding whether the proof of the first mechanism is acceptable, depending upon the results of the verifying section and checking section". Patent claims recite "storing a designated operation scheme, two input numbers ....memory" which encompasses the

instant application claims "a memory for storing an evaluation result of the proof system obtained by the distinguisher". Thus patent claims anticipate the instant claims.

Claims of the instant application are anticipated by patent claims in that the patent claims contains all the limitations of the instant application. Claims of the instant application therefore is not patentably distinct from the earlier patent claims and as such are unpatentable for obvious-type double patenting *(In re Goodman (CAFC) 29 USPQ2d 2010 (12/3/1993).*

**5.** Claims 1 – 11 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 – 18 of U.S. Patent No. 7,035,404. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1 – 11 correspond to the claims of 1 – 18 of the patent claims, except in the instant claims the elements "a proof system comprising a prover supplied with a first random tape and a verifier supplied with a second random tape, wherein the prover communicates with the verifier to prove that the prover has a witness comprising: a generator supplied with a third random tape ... a simulator with a fourth random tape, a distinguisher supplied with a fifth random tape, wherein the generator supplies the common input to the prover, the verifier, the simulator and the distinguisher ...the distinguisher evaluates the proof system .... and computationally indistinguishable for at least one of possible common inputs" is referred in the patent claims as "generating processing of generating output ...response generating processing of generating a response ... processing of outputting said transformation information ...". Thus patent claims anticipate the instant claims.

Claims of the instant application are anticipated by patent claims in that the patent claims contains all the limitations of the instant application. Claims of the instant application therefore is not patentably distinct from the earlier patent claims and as such are unpatentable for obvious-type double patenting *(In re Goodman (CAFC) 29 USPQ2d 2010 (12/3/1993).*

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

**6.** Claims 1 – 11 are rejected under 35 U.S.C. 102(b) as being anticipated by Kanda et al. (US Patent 6,011,848).

**7.** As per Claims 1 and 7 – 11, Kanda teaches "A proof system comprising a prover supplied with a first random tape and a verifier supplied with a second random tape, wherein the prover communicates with the verifier to prove that the prover has a witness, comprising: a generator supplied with a third random tape, for generating a common input comprising g, h, y, and z' and a witness comprising x from the third random tape, wherein x is an integer and g, h and z' are elements of a group which is previously determined and has an order thereof, wherein the prover inputs the common input and the witness from the generator and the verifier inputs the common input from the generator; wherein, after interaction between the verifier and the prover starts, the

following steps are performed: A) the verifier uniformly and randomly selects an integer b smaller than the order of the group and a challenge c from the second random tape, generates a challenge commitment a, and sends the challenge commitment a to the prover;

B) the prover uses the first random tape to uniformly and randomly select d, e and f, which are integers smaller than the order of the group, calculates h', w', v, y', v', h", and w" and sends h', w', v, y', v', h" and w" to the verifier;

C) the verifier sends the integer b and the challenge c to the prover;

D) the prover determines from the received b and c whether a is satisfied and, if not satisfied, then the interaction is terminated and, if satisfied, then the interaction continues;

E) the prover uses the integers d, e and f and the witness to calculate response r and r' and send them to the verifier: r (the order of the group); and r' (the order of the group);

F) the verifier uses the h', w', v, y', v', h" and w" received from the prover, the response r and r', the challenge c, and the common input p, q, g, h, y, z' to determine whether a set of following expressions is satisfied ... and, if the set of following expressions is satisfied, then the verifier accepts the proof and, if at least one expression is not satisfied, then the verifier denies the proof" (Column 6 line 21 – Column 8 line 41).

**8.** As per Claims 2 and 3, Kanda teaches "wherein the prover comprises a proving section and a hash function section, wherein the hash function section inputs data from the proving section and outputs hash data of the inputted data back to the proving section, the proof history is generated by the prover in which the proving section interacts with the hash function section to produce interactive data and hash data of the interactive data is replaced with random data, wherein the proof history further includes data transferred from the prover to the verifier, the simulated proof history is generated by the simulator that simulates interaction between the prover and the verifier based on the common input and the fourth random tape, the simulated proof history including the simulated interactive data" (Column 6 line 21 – Column 8 line 41).

**9.** As per Claim 4, Kanda teaches "wherein, if for every distinguisher a difference in distribution between the proof history and the simulated proof history is computationally indistinguishable for a great majority of possible common inputs to an extent of an approximately 100% probability and computationally distinguishable for the remaining part of the common inputs, it is determined that the proof system is classified under a weakly computational zero-knowledge proof class" (Column 6 line 21 – Column 8 line 41).

**10.** As per Claims 5 and 6, Kanda teaches "a memory for storing an evaluation result of the proof system obtained by the distinguisher, wherein the evaluation result is on public view" and "wherein the evaluation result stored in the memory is accessible through a network" (Column 10 line 49 – Column 11 line 21).

***Conclusion***

**11.** Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

**12.** The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-232-4195. Any inquiry of a general nature or

relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
August 29, 2007.

Substitute for Form 1449 A & B/PTO

# INFORMATION DISCLOSURE STATEMENT BY APPLICANT

*(use as many sheets as necessary)*



| Sheet | 1 | of | 1 |
|---|---|---|---|

| *Complete if Known* | |
|---|---|
| Application Number | 10/718,663 |
| Confirmation Number | 1253 |
| Filing Date | November 24, 2003 |
| First Named Inventor | Jun FURUKAWA |
| Art Unit | 2131 |
| Examiner Name | Unknown |
| Attorney Docket Number | Q78522 |

## FOREIGN PATENT DOCUMENTS

| Examiner Initials* | Cite No.[1] | Foreign Patent Document: Country Code[3] | Foreign Patent Document: Number[4] | Foreign Patent Document: Kind Code[5] (if known) | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Translation[6] |
|---|---|---|---|---|---|---|---|
| /PP/ | | JP | 2001-251289 | A | 09-14-2001 | | No |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

## NON PATENT LITERATURE DOCUMENTS

| Examiner Initials* | Cite No.[1] | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city, and/or country where published. | Translation[6] |
|---|---|---|---|
| | | ~~Sangyo Tosyo Shuppan, "Modern Cryptography", July 30, 1997, pages 131-150.~~ | |
| /PP/ | | Oded Goldreich, Cambridge, "Foundation of Cryptography", July 30, 1997, pages 184-330. | |
| | | | |
| | | | |
| | | | |
| | | | |

| Examiner Signature | /Pramila Parthasarathy/ | Date Considered | 08/28/2007 |
|---|---|---|---|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]See Kind Codes of USPTO Patent Documents at www.uspto.gov, MPEP 901.04 or in the comment box of this document. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST. 3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to indicate here if English language Translation is attached.